VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

Fakulta elektrotechniky
a komunikačních technologií

SEMESTRÁLNÍ PRÁCE

Brno, 2019 Bc. Juraj Korček

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
BRNO UNIVERSITY OF TECHNOLOGY

FAKULTA ELEKTROTECHNIKY A KOMUNIKAČNÍCH TECHNOLOGIÍ
FACULTY OF ELECTRICAL ENGINEERING AND COMMUNICATION

ÚSTAV TELEKOMUNIKACÍ
DEPARTMENT OF TELECOMMUNICATIONS

APLIKACE PRO GENEROVÁNÍ A OVĚŘOVÁNÍ KONFIGURACÍ SÍŤOVÝCH ZAŘÍZENÍ
APPLICATION GENERATING AND VERIFYING CONFIGURATIONS OF NETWORK DEVICES

SEMESTRÁLNÍ PRÁCE
SEMESTRAL THESIS

AUTOR PRÁCE — **Bc. Juraj Korček**
AUTHOR

VEDOUCÍ PRÁCE — **doc. Ing. Jan Jeřábek, Ph.D.**
SUPERVISOR

BRNO 2019

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
FAKULTA ELEKTROTECHNIKY A KOMUNIKAČNÍCH TECHNOLOGIÍ

Semestrální práce

magisterský navazující studijní obor **Informační bezpečnost**
Ústav telekomunikací

Student: Bc. Juraj Korček ***ID:*** 187238
Ročník: 2 ***Akademický rok:*** 2019/20

NÁZEV TÉMATU:

Aplikace pro generování a ověřování konfigurací síťových zařízení

POKYNY PRO VYPRACOVÁNÍ:

Seznamte se s problematikou síťových zařízení, síťových operačních systémů, hlavních používaných komunikačních protokolů a způsobů konfigurace těchto zařízení. Dále prostudujte problematiku osvědčených postupů konfigurace, zejména s ohledem na bezpečnost fungování zařízení v síti a také problematiku anonymizace těchto konfigurací. Navrhněte systém či aplikaci, která bude umět pro vybranou množinu síťových zařízení vytvářet přednastavené parametry nastavení, které bude možné na dané síťové zařízení aplikovat. Dále musí daná aplikace umět verifikovat správnost existujících konfigurací, upozornit na případné nedostatky a i konfiguraci modifikovat tak, aby splňovala hlavní bezpečnostní a provozní standardy a doporučení. Fungování aplikace ověřte na testovacích vzorcích síťových konfigurací různých zařízení z několika různých sítí a případně i různých výrobců.
V rámci semestrálního projektu je třeba vypracovat teoretickou část zadání, vybrat vhodné programovací prostředí pro plánovanou aplikaci a navrhnout a popsat strukturu dané aplikace či systému, včetně základního popisu jednotlivých komponent a jejich předpokládané funkcionality. Vlastní řešení mírně rozpracujte.

DOPORUČENÁ LITERATURA:

[1] Stallings W., Network security essentials: applications and standards. 6th ed. Hoboken: Pearson education, 2017, 445 s. ISBN 978-0-13-452733-8.

[2] McMillan, T., CCNA Security Study Guide: Exam 210-260. 2nd ed. USA: Sybex, 2018, 384 s. ISBN 978-1--1-940993-9.

Termín zadání: 23.9.2019 ***Termín odevzdání:*** 21.12.2019

Vedoucí práce: doc. Ing. Jan Jeřábek, Ph.D.
Konzultant:

prof. Ing. Jiří Mišurec, CSc.
předseda oborové rady

VYHLÁSENIE

Vyhlasujem, že svoju semestrálnú prácu na tému „Aplikace pro generování a ověřování konfigurací síťových zařízení“ som vypracoval samostatne pod vedením vedúceho semestrálnej práce, s využitím odbornej literatúry a ďalších informačných zdrojov, ktoré sú všetky citované v práci a uvedené v zozname literatúry na konci práce.

Ako autor uvedenej semestrálnej práce ďalej vyhlasujem, že v súvislosti s vytvorením tejto semestrálnej práce som neporušil autorské práva tretích osôb, najmä som nezasiahol nedovoleným spôsobom do cudzích autorských práv osobnostných a/alebo majetkových a som si plne vedomý následkov porušenia ustanovenia § 11 a nasledujúcich autorského zákona Českej republiky č. 121/2000 Sb., o práve autorskom, o právach súvisiacich s právom autorským a o zmene niektorých zákonov (autorský zákon), v znení neskorších predpisov, vrátane možných trestnoprávnych dôsledkov vyplývajúcich z ustanovenia časti druhej, hlavy VI. diel 4 Trestného zákonníka Českej republiky č. 40/2009 Sb.

Brno ....

podpis autora

Obsah

Zoznam obrázkov

Zoznam tabuliek

Zoznam výpisov

Úvod

Kybernetická bezpečnosť je bezpochyby jednou z hlavných tém 21. storočia. Útoky na infraštruktúru a systémy naberajú nielen na frekvencii, ale čo je ešte horšie na sofistikovanosti. Napriek častému zdôrazňovaniu odborníkov o kladenie čoraz väčšieho dôrazu na bezpečnosť pri návrhu, implementácii a nasadeniu, sa stále stretávame s fatálnymi dôsledkami, ktoré boli spôsobené nedostatočným venovaním pozornosti bezpečnosti.

Problém nedostatočného zabezpečenia nie je ani tak nevedomosť základných bezpečnostných praktík administrátorov alebo programátorov, ale potreba rýchleho nasadenia systému a infraštruktúry s odložením implementácie bezpečnostných praktík na neskôr. Tieto problémy vznikajú aj pri dodatočnej implementácií nových modulov a pridaní novej infraštruktúry, kedy sa nemení celok, ale pridanie jednej časti môže výrazne ovplyvniť a zmeniť stav bezpečnosti celého systému. Z tohto dôvodu je priam žiadúce disponovať nejakým procesom alebo nástrojom na dodatočné zistenie nedostatkov a ich následnú elimináciu. Veľmi silnou motiváciou by malo byť aj to, že dôsledkom bezpečnostných nedostatkov sú globálne miliardové škody a straty reputácií firiem.

Jednou z hlavných častí infraštruktúry, kde dochádza k významným bezpečnostným incidentom je počítačová sieť, bez ktorej by dnes informačné technológie nevedeli fungovať. Preto sa táto práca bude zaoberať práve ňou, keďže je vstupnou bránou do systémov a jej vyradením alebo zneužitím prichádzajú organizácie o finančné prostriedky, citlivé dáta a dôveru užívateľov.

Výsledkom tejto práce bude aplikácia overujúca nastavenia sieťových zariadení prevažne v lokálnej sieti, ktorá umožňuje zjednať nápravu na základe nájdených nedostatkov. Výhodou oproti existujúcim riešeniam bude otvorenosť kódu a modularita, ktorá umožní rozšírenie aplikácie na sieťové zariadenia rôznych výrobcov. Dôležitým výstupom bude taktiež zoznam bezpečnostných a prevádzkových odporučaní vychádzajúcich z rôznych štandardov a odporučaní, ktoré môžu byť v budúcnosti použité ďalšími užívateľmi aplikácie pri zostavovaní modulov pre zariadenia rôznych výrobcov. Jednou z kľúčových vlastností je bezplatnosť, keďže podľa zistení takmer polovica útokov smeruje na malé firmy, ktoré bezpečnosť často neriešia z finančnej náročnosti programov na detekciu bezpečnostných nedostatkov.

1 Kybernetická bezpečnosť

S čoraz na väčšou informatizáciou naprieč všetkými odvetviami života, je nutnosťou riešiť aj zabezpečenie systémov, infraštruktúry a dát. Kybernetická bezpečnosť je bez pochýb jednou z najdiskutovanejších tém 21. storočia.

Podľa zistení z roku 2018 [1] takmer polovica útokov smeruje na malé firmy, ktoré bezpečnosť riešia iba minimálne alebo vôbec. Predpokladá sa [1], že pre rok 2019 bude na kybernetickú bezpečnosť minutých 6 miliárd dolárov, naopak škody spôsobené kybernetickými útokmi presiahnu jednu miliardu dolárov a veľmi záškodné útoky typu *Distributed Denial of Service – distribuované odoprenie služby* (DDoS) by mali vzrásť až šesťnásobne.

Vyššie zmienené predpovede len potvrdzujú dôležitosť kybernetickej bezpečnosti pri návrhu, implementácie, nasadzovaní a prevádzke informačných technológií.

1.1 Vybrané pojmy z kybernetickej bezpečnosti

- Informačné aktívum (Asset) – čokolvek, čo je nutné chránit, napr. dáta, fyzická informačná infraštruktúra, systémy [3].

- Zraniteľnosť (Vulnerability) – neprítomnosť alebo nedostatočné opatrenia na zabezpečenie. Zraniteľnosť môže byť prítomná hardvéri, softvéri alebo samotnom užívateľovi [3].

- Hrozba (Threat) – vzniká v prípade odhalenia alebo zneužitia zraniteľnosti. Zároveň platí, že hrozbou je aj zraniteľnosť, ktorá doposiaľ nebola neidentifikovaná [3].

- Útočník (Threat agent) – entita, ktorá zneužije zraniteľnosť [3].

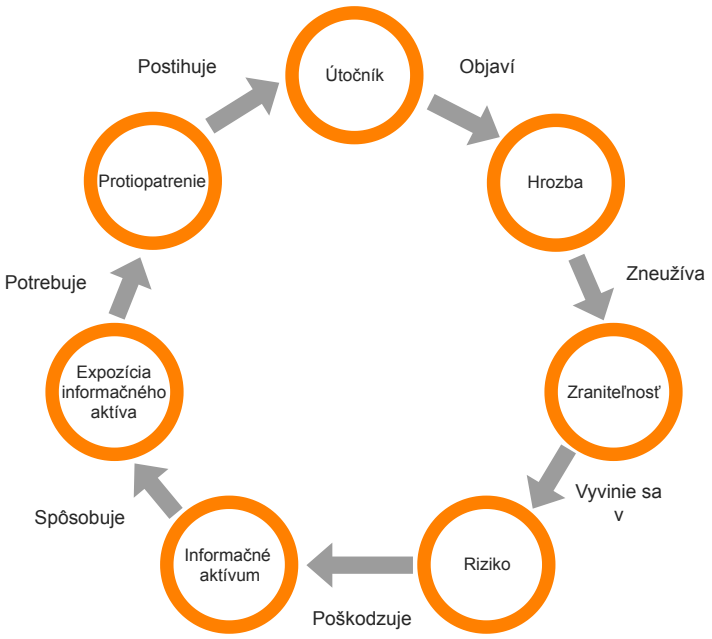
- Riziko (Risk) – pravdepodobnosť, že útočník využije zraniteľnosť, pričom príde k dopadu na systém alebo infraštruktúru [3].

- Útok na bezpečnosť (Security attack/Explotation) – krok, ktorý kompromituje bezpečnosť informačného aktíva [2].

- Bezpečnostný mechanizmus (Security mechanism) – proces, ktorý je navrhnutý na detegovanie, prevenciu a zotavenie z útoku na bezpečnosť.

- Protiopatrenie (Countermeasure) – ochranné opatrenie, ktoré znižuje riziko [3].

- Expozícia informačného aktíva (Exposure) – dochádza k nej ak je aktívum vystavené stratám nedostatočným alebo neprítomným zabezpečením [3].



Obr. 1.1: Koncept bezpečnosti a vzájomné vzťahy pojmov [3]

Na obrázku 1.1 je možné vidieť vzájomnú interakciu medzi pojmami. Zároveň je nutné si uvedomiť, že takýto cyklus nie je v systéme alebo infraštruktúre jeden a taktiež môže vzniknúť niekoľko paralelných cyklov pričom každý môže mať počiatok v inom uzle. Je dobré myslieť na to, že jednotlivé cykly môžu na seba vplývať, napríklad jedno protiopatrenie môže postihnúť viacero útočníkov využívajúcich rôzne hrozby.

1.2 Ciele sieťovej bezpečnosti

Bezpečnosť počítačovej siete, tak ako aj iných podoblastí kybernetickej bezpečnosti je založená na troch základných princípoch známych ako *confidentiality, integrity, availability – dôvernosť, integrita, dostupnosť* (CIA). Bezpečnosť musí pokryť všetky tri aspekty popísané týmto modelom, pričom narušenie čo i len jednej zložky má za následok nesplnenie celkového zabezpečenia [2].

1.2.1 Triáda CIA

Triáda CIA pozostáva z nasledujúcich častí [3]:

- Confidentiality (Dôvernosť) – zabránenie prístupu k dátam alebo informáciám neoprávneným osobám. Na zaistenie tejto požiadavky sa najčastejšie používa šifrovanie, ale aj autentizácia a autorizácia. Jej strata vedie k neoprávnenému zverejnenie informácií.
- Integrity (Integrita) – dáta alebo informácie sú zabezpečené proti neautorizovanej modifikácií a poškodeniu. Týmto zaisťujem konzistenciu dát pri prenose alebo uchovaní na médiu. Integritu zaisťujeme hašovacími funkciami prípadne za pomoci *Access Control List – zoznam pre riadenie prístupu* (ACL).
- Availability (Dostupnosť) – dáta alebo informácie sú dostupné iba pre určité entity v daný čas a miesto.

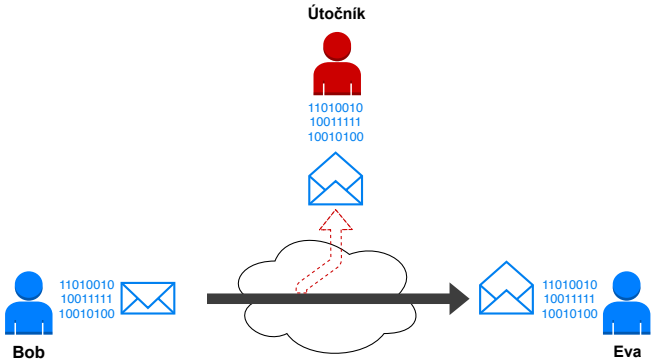
Obr. 1.2: Triáda dôvernosť, integrita a dostupnosť demonštrujúca potrebu všetkých troch prvkov na zaistenie bezpečnosti [2]

Aj keď triáda CIA definuje ciele na zaistenie bezpečnosti, tak niektorí odborníci ju nepovažujú za dostatočnú a zavádzajú ďalšie dve podmienky a pojmy [4]:

- Authencity (Autenticita) – overenie originálnosti a platnosti správy a identity jej pôvodcovi. Najčastejšie sa na zaistenie tejto podmienky využívajú certifikáty.
- Accountability (Sledovateľnosť) – identifikácia prístupu k informáciám a vysledovateľnosť bezpečnostných incidentov v prípade využitia forenznej analýzy. Väčšinou je táto požiadavka zaistená záznamom činnosti v systéme formou logu.

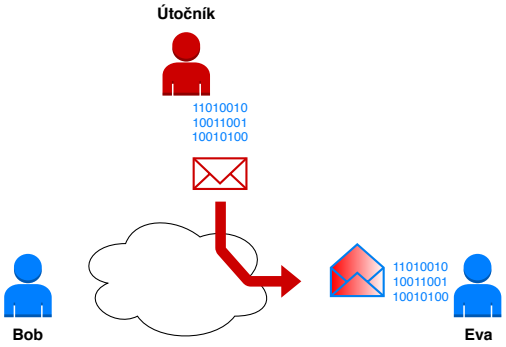
1.3 Pasívne a aktívne útoky

Útoky na bezpečnosť môžu byť rozdelené do dvoch skupín [2]. Jednou skupinou je pasívny útok, kde nepozmeňuje útočník pôvodné dáta a nevplýva na príjemcu týchto dát. Druhou možnosťou je aktívny útok, pri ktorom sú buď pozmenené dáta doručené príjemcovi alebo je obeť nejakým spôsobom ovplyvňovaná, napríklad zasielaním falošných informácií.

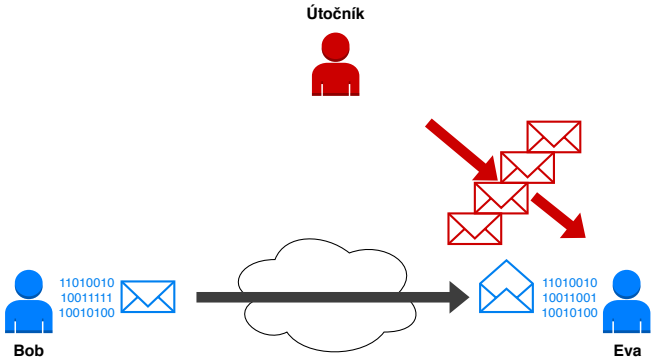


Obr. 1.3: Príklad pasívneho útok, pri ktorom útočník odpočúva komunikáciu medzi dvoma uzlami [4]

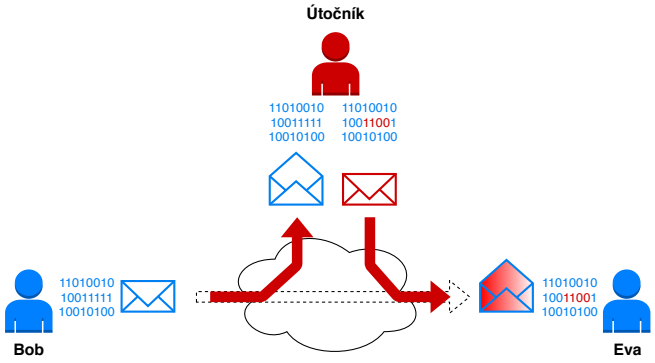
Pri pasívnom útoku, ktorý je znázornený na obrázku 1.3 ide útočníkovi prevažne o zachytenie prenášanej komunikácie a monitorovanie a analýzu prevádzky. Odposluch a zobrazenie obsahu dát je účinné hlavne pri nepoužití šifrovania správ medzi koncovými bodmi alebo aj pri použití slabých šifier, krátkych kľúčov a nedostatočne bezpečných hesiel. Monitorovanie prevádzky, respektíve analýza komunikácie je možná aj pri použití šifrovania, keďže každá komunikácia je charakteristická určitým vzorom. Pasívne útoky je nesmierne obtiažne detegovať nakoľko nemodifikujú dáta pri prenose. Najúčinnejšia obrana je použitie dostatočne silných šifier na zabezpečenie dát. Jeden z pasívnych útokov sa hojne využíva aj pri prevencii v *Intrusion Detection System – systém detekcie narušenia* (IDS) a *Intrusion Prevention System – systém prevencie prienikov* (IPS), kde bez analýzy prevádzky by nebolo možné zabezpečiť sieť. Pasívnymi útokmi sa nespôsobuje škoda na systéme alebo infraštruktúre, ale hrozba spočíva v narušení dôvernosti.



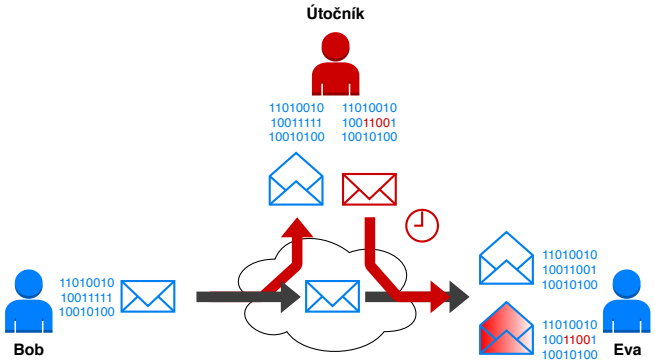
Obr. 1.4: Príklad aktívneho útoku maškarádou, kedy uzol Eva obdrží falošnú správu od útočníka mysliac si, že ide o správu od uzla Bob [4]



Obr. 1.5: Príklad aktívneho útoku DOS, pri ktorom je uzol Eva zahltený nevyžiadanými správami (označené červeno) [4]



Obr. 1.6: Príklad aktívneho útoku modifikáciou správy, pri ktorom je originálna správa presmerovaná cez útočníka, následne pozmenená a prijatá uzlom Eva, ktorý ju považuje za legitímnu [4]



Obr. 1.7: Príklad aktívneho útoku prehratím, pri ktorom príde uzlu Eva legitímna správa (označená modro) a následne po určitom čase aj odchytená správa od útočníka, ktorá je pozmenená (označená červeno) [4]

Aktívne útoky sú sofistikovanejšie ako pasívne, modifikujú dáta alebo vytvárajú falošné, o ktorých prijímateľ predpokladá, že prišli od zdroja, s ktorým pôvodne komunikoval. Hrozby, ktoré môžu týmito útokmi nastať sú strata integrity, teda modifikácia dát a ohrozenie dostupnosti pričom vždy dochádza ku škode na systéme alebo infraštruktúre. Maškaráda je prvým z aktívnych útokov, kde ako je možné vidieť na obrázku 1.4, útočník vytvára falošnú správu, ktorú zasiela obeti a tá sa domnieva, že komunikuje s pôvodným zdrojom, v našom prípade Bobom. Použitím osobných certifikátov na oboch stranách by bolo možné odhaliť, že správa nepochádza od zdroja, ale od útočníka. Príkladom aktívneho útoku je aj útok odoprenia služby 1.5, kde sa vytvárajú falošné dáta generované vysokou frekvenciou za účelom odstaviť systém alebo infraštruktúru, ktorá nezvláda spracovanie toľkých požiadaviek, keďže nebola na takúto záťaž dimenzovaná. Tretím aktívnym útokom 1.6 je modifikácia správy útočníkom pri prechode komunikačným kanálom, ktorý sa realizuje rôznymi technikami podvrhnutia zdroja alebo identity. Komunikácia v tomto prípade prebieha cez útočníka, ktorý tento útok mohol uskutočniť napríklad podvrhnutím smerovania. Posledným útokom je útok prehratím 1.7, čo je útok veľmi podobný predchádzajúcemu, akurát obeť obdrží najprv pôvodnú nepozmenenú správu a následne po určitom čase aj modifikovanú správu od útočníka. Takéto správy môžu byť generované aj ako nežiadúca sieťová prevádzka pri zahltení prvkov alebo pri zlom nastavení smerovania. Citlivé sú najmä tranzakčné systémy napríklad databáze. Zabrániť tomuto útoku je možné pomocou časových pečiatok a jednoznačných identifikátorov.

2 Bezpečnostný audit

Auditovanie je veľmi dôležitým prvkom správy informačných systémov a infraštruktúry, pretože umožňuje zaistiť bezpečnosť týchto informačných aktív porovnávaním s vytvorenými štandardmi, odporúčaniami a predpismi. Zaoberá sa otázkami čo a ako zabezpečiť, vyhodnocovaním a riadením rizík a následným dokazovaním, že náprava znížila riziko hrozby.

Auditovanie sa skladá z piatich pilierov [5]:

1. Posúdenie
2. Prevencia
3. Detekcia
4. Reakcia
5. Zotavenie

Pri posudzovaní si je potreba klásť otázky či sú prístupové práva dostatočne špecifikované, aká je pravdepodobnosť útoku na zraniteľnosť a podobne. Prevencia nespočíva iba v technológiách ako firewall prípadne IDS a IPS, ale aj v politikách, procesoch a povedomí o probléme. Detekcia a reakcia spolu úzko súvisia a je potrebné skrátiť dobu medzi týmito dvoma bodmi, bez dôkladnej detekcie nie je možné vykonať reakciu. Mnohé reakcie na detekciu problému sú už rôznymi technológiami implementované automatizovane. Posledný článkom je zotavenie, ktoré je dôležité pri službách vysokej dostupnosti. Výborným príkladom detekcie, reakcie a zotavenia z problému sú protokoly z rodiny *First Hop Redundancy Protocol* (FHRP).

Proces auditu pozostáva z niekoľkých fází: [5]

1. Plánovanie – stanovenie cieľov a predmetu auditu. Definuje sa rozsah, teda čo všetko je v pláne auditom pokryť.
2. Výskum – vytváranie auditného plánu na základe štandardov a odporúčaní a špeciálnych expertíz. Kontaktujú sa tiež dotknuté strany, ktoré nám môžu byť nápomocné pri plnení cieľov.
3. Zbieranie dát – vyžiadanie potrebných podkladov a dát na vykonanie auditu, zozbieranie dôkazov. V tejto fáze sa tiež vyberajú rôzne softvérové nástroje na vykonanie auditu a vytvorí sa checklist na základe auditného plánu a zozbieraných dôkazov.
4. Analýza dát – posúdenie všetkých dôkazových dát pomocou checklistu a softvéru na podporu auditu. Na základe nájdených nedostatkov sa vytvoria odporúčania, ktoré by mali znížiť riziká hrozieb.
5. Vytváranie správy – súpis nájdených nedostatkov, možných riešení na zníženie rizík do auditnej správy a prezentácia tejto správy dotknutým stranám.

6. Aplikácia opatrení – nasadenie a použitie protiopatrení prezentovaných alebo vyplývajúcich z auditnej správy. Následne sa môže vykonať monitorovanie a hlásenie o úspešnosti zmien.

Typy auditov podľa zistení, hĺbky a rozsahu auditu:

- Bezpečnostná kontrola – je najzákladnejšia forma analýzy bezpečnosti, na základe ktorej sa následne formujú ďalšie aktivity na zaistenie bezpečnosti. Do tejto kategórie spadajú automatizované nástroje na skenovanie zraniteľností a penetračné nástroje, ktoré generujú zoznam potenciálnych zraniteľností, ale je potrebné ďalšie podrobnejšie preskúmanie výsledkov a zistení a stanovenie, ako sa k ním zachovať. Patria sem nástroje ako napríklad Nmap, Nessus a podobne. Za bezpečnostnú kontrolu možno považovať preskúmanie politík alebo architektúry daného systému a infraštruktúry. Dá sa povedať, že ide o akýsi rýchly náhľad na bezpečnosť, ktorého výstupom je poznanie a identifikovanie problému.
- Hodnotenie bezpečnosti – je ďalším stupňom, pričom ide o podrobnejší pohľad na problém z profesionálnejšieho hľadiska. Kvalifikuje sa riziko k jednotlivým zisteniam a stanovuje sa relevantnosť a kritickosť týchto zistení na konkrétnu organizáciu a prípad použitia.
- Bezpečnostný audit – je štandardizovanou a najdôkladnejšou formou posúdenia bezpečnosti. Bezpečnosť sa porovnáva so štandardmi alebo benchmark-mi, v niektorých prípadoch aj s predpismi dohliadahúcich orgánov. Výsledkom je posúdenie, na koľko je organizácia alebo skúmaný objekt v zhode s porovnávaným štandardom. Typickým príkladom štandardov sú ISO27001 a COBIT.

2.1 Manažment rizík

Manažment rizík je proces pozostávajúci z analýzy rizík a riadenia rizík [3]. Dôležitým faktom je, že riziko nie je možné eliminovať, ale ho iba znížiť.

Pri analýze rizík zisťujeme, aké riziká existujú, ako medzi sebou súvisia a aké škody môžu spôsobiť. Analýza rizík môže byť vykonávaná kvalitatívne a kvantitatívne.

Štandard NIST SP 800-30 [6] definuje nasledujúce kroky pri analýze rizík:

1. Identifikácia informačných aktív a ich význam
2. Identifikácia hrozieb
3. Identifikácia zraniteľností
4. Analýza riadenia a kontroly
5. Zistenie pravdepodobnosti
6. Identifikovanie dopadu
7. Definovanie rizika ako súčinu pravdepodobnosti a dopadu
8. Odporúčanie na zavedenie riadenia a kontroly na zníženie rizika
9. Zdokumentovanie výsledkov

Riadenie rizík má za úlohu minimalizáciu potenciálnych škôd odhalených pri analýze rizík s ohľadom na vyváženie nákladov na riadenie rizika.

Prístupy k nájdenému riziku [2][3][5]:

- Vyhnutie sa riziku – je uplatnené ak prítomnosť a funkčnosť informačného aktíva nestojí za podstúpenie rizika, a teda toto aktívum vôbec nepoužijeme. Napríklad vypnutie menej bezpečných a nevyužívaných sieťových služieb.
- Zníženie – aplikovanie protiopatrenia na odstránenie hrozby alebo zraniteľnosti prípadne zníženie pravdepodobnosti rizika. Nikdy nie je však možné riziko eliminovať. Príkladom môže byť obmedzenie prístupu k sieťovému prvku.
- Akceptovanie – v prípade neexistujúceho protiopatrenia alebo veľmi nízkeho rizika. Častokrát ide o bezpečnostnú chybu softvéru v službe, ktorú využívame a nie je možné ju vypnúť ani aplikovať protiopatrenie.
- Presun – riziko je možné presunúť na inú organizáciu, napr. poistenie v prípade škody spôsobenej nedostatočným zabezpečením.
- Ignorácia – úplné vypustenie faktu, že dochádza k riziku, tento prístup sa považuje za iracionálny.

Na ohodnotenie rizika slúžia rôzne systémy hodnotenia, jedným z nich je *Common Vulnerability Scoring System* (CVSS), ktorý definuje riziká podľa definovaných metrík na základe dosiahnutého skóre do nasledujúcich tried:

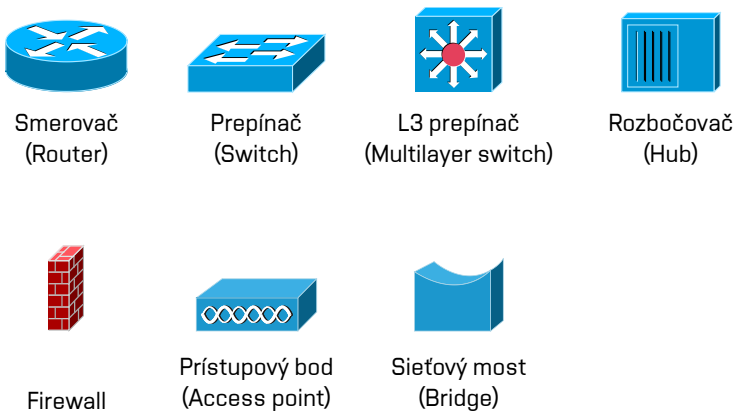
- 0: No issue
- 0,1 – 3,9: Low
- 4,0 – 6,9: Medium
- 7,0 – 8,9: High
- 9,0 – 10,0: Critical

3 Prevádzka a bezpečnosť sietí

Prevádzka sieťových zariadení je proces nielen o monitorovaní incidentov, zabezpečovaní konzistencie a konvergencie siete, ale aj o aktualizáciách softvéru a hardvéru, aplikovaní bezpečnostných zásad a politík. Táto kapitola preto opisuje jednotlivé aspekty s ktorými sa pri prevádzke siete môžeme stretnúť.

3.1 Sieťové prvky

Medzi základné stavebné piliere sietí, bez ktorých nie je možná komunikácia koncových staníc patria smerovače (router) a prepínače (switch). Mimo týchto dvoch základných zariadení sa v *Local Area Network* (LAN) sieťach často vyskytujú prístupové body (access point), firewally, sieťové mosty (bridge) a v dnes už ojedinelých prípadoch ešte aj rozbočovače (hub). V súčasnosti však jedno zariadenie môže kombinovať funkcie zariadení, ktoré majú podľa modelov TCP/IP alebo ISO/OSI na starosti inú vrstvu modelu. Preto sa dnes hlavne z finančných dôvodov používajú takzvané L3 prepínače, ktoré s určitými obmedzeniami vedia nahradiť nákladné smerovače. Taktiež smerovače ako aj L3 prepínače umožňujú filtrovanie paketov, takže vedia čiastočne zastať aj základné funkcie firewallu. Značky najpoužívanejších sieťových zariadení su vyobrazené na obrázku 3.2 a budú používané v nasledujúcich kapitolách.



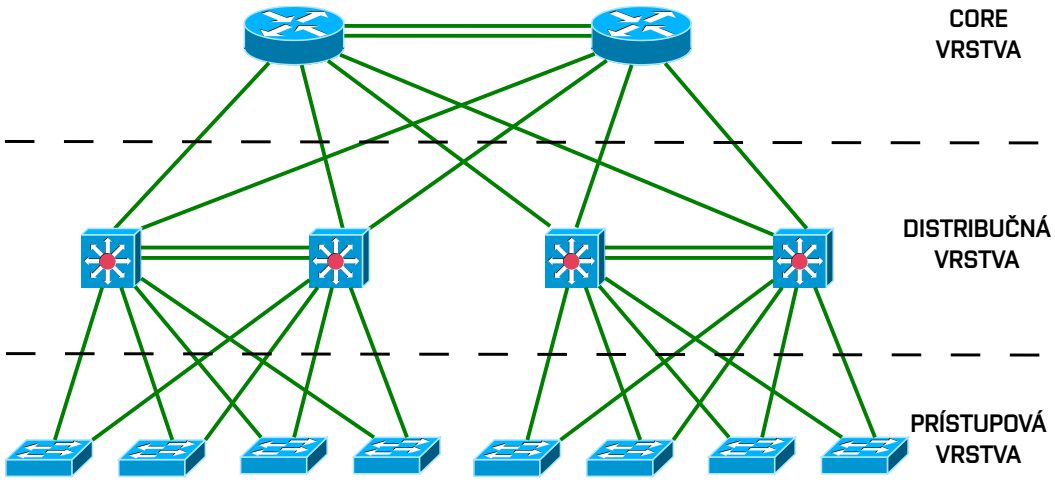
Obr. 3.1: Typy sieťových zariadení v lokálnych sieťach

3.2 Hierarchický model sietí

S postupným nárastom sieťových zariadení a komplexnosti siete dochádza v sieťach bez hierarchie k mnohým problémom ako veľké broadcast domény, vysoká cena za port, vysoké zaťaženia zariadení, neprítomnosť redundancie. Preto sa zaviedol hierarchický model siete, ktorý rieši problémy veľkosti a rozsahu broadcast a kolíznych domén, umožňuje efektívne prideľovanie *Internet Protocol* (IP) adries a oddeľuje zariadenia pracujúce na jednotlivých vrstvách ISO/OSI.

Siete sú spravidla delené do 3 vrstiev s definovanými funkciami [8]:

- Core – tvorí vysokorýchlostnú chrbticu siete, agreguje dáta z distribučnej vrstvy a mala by byť redundantná. Nároky na rýchlosť portov a výkon zariadenia sú obzvlášť vysoké, a preto sa využívajú prevažne smerovače, ale taktiež ako v distribučnej vrstve dnes už aj L3 prepínače.
- Distribučná (Distribution) – agreguje dáta z prístupovej vrstvy, vytvára a oddeľuje broadcast domény, riadi smerovanie medzi *Virtual LAN* (VLAN) a filtrovanie paketov. Táto vrstva kvôli zabezpečeniu dostupnosti využíva agregovanie a redundanciu liniek. Typicky sa skladá zo smerovačov, no v dnešnej dobe hlavne z L3 prepínačov, keďže tie nie sú finančne také náročné.
- Prístupová (Access) – vstupný bod do siete, ktorý riadi prístup a politiku pre koncové zariadenia, segmentuje sieť, vytvára a separuje kolízne domény. V neposlednej rade zariaďujú prístup k distribučnej vrstve. Je tvorená zariadeniami ako prepínač, rozbočovač alebo prístupový bod.



Obr. 3.2: Hierarchické rozdelenie siete na vrstvy

V menších sieťach prevažne malých firiem sa využíva zlučovanie vrstiev nazývaných ako collapsed core, ktoré zlučujú distribučnú a core vrstvu, prípadne zlučujú všetky tri vrstvy dokopy.

Cieľom hierarchického modelu a dobre navrhnutej siete je dosiahnutie nasledujúcich vlastností:

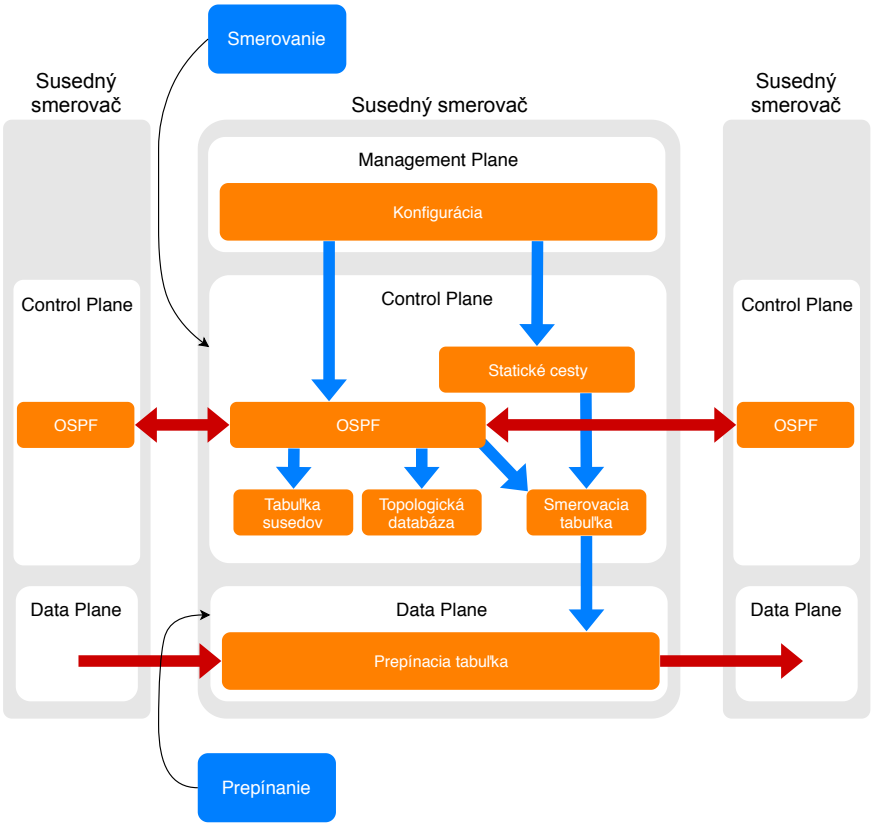
- Škálovateľnosť – jednoduché a bezproblémové pridanie zariadenia pri raste a rozširovaní siete.
- Redundancia – zabezpečenie vysokej dostupnosti viacnásobnými linkami medzi zariadeniami a zálohovanie samotných zariadení ich redundanciou.
- Výkonnosť – agregovanie liniek a výber dostatočne výkonných zariadení
- Bezpečnosť – zabezpečenie siete na viacerých úrovniach ako napríklad portoch, oddelením segmentov pomocou VLAN, riadením prístupu, šifrovaním a pod.
- Manažovateľnosť – vytvorenie šablón, definovaných štandardov a pravidiel na zaistenie konzistentnosti konfigurácií zariadení na jednoduchšie odhaľovanie chýb.
- Udržovateľnosť – schopnosť systému prechádzať zmenami komponentov, služieb a vlastností.

3.3 Funkčné roviny sieťových prvkov

Sieťové prvky sú zodpovedné nielen za preposielanie dát medzi koncovými stanicami, ale aj za mnohé riadiace dáta medzi sebou, bez ktorých by sieť nebola funkčná. Preto sa jednotlivé protokoly a služby rozdeľujú troch rovín, a to management, control a data plane. Tieto pojmy sa využívajú vo väčšej miere v softvérovo definovaných sieťach, no sú platné aj v klasickej koncepcii.

Rovina management je zodpovedná za konfiguráciu a správu zariadení a riadenie prístupu ku konfiguráciám. Typickými príkladmi protokolov pracujúcich na tejto rovine sú *Simple Network Management Protocol* (SNMP), *Authentication Authorization Accounting* (AAA), Syslog, *Secure Shel* (SSH) a mnohé ďalšie [7]. Druhá rovina, control plane má na starosti prevažne riadenie siete a smerovanie. Zaoberá sa otázkou kadiaľ budú pakety smerované a prenáša riadiace a signalizačné informácie pre protokoly ako napríklad, *Open Shortest Path First* (OSPF), Spanning tree, FHRP [7]. Poslednou rovina je data plane nazývaná často aj forwarding plane, ktorá prepína pakety na daný port na základe rozhodnutia z control plane. Táto časť sieťových prvkov musí byť veľmi rýchla, aby zaistila nízku odozvu a dostatočne vysoké prenosové rýchlosti. Nižšie uvedený obrázok 3.3 reflektuje tok dát z jednej roviny do druhej a tiež medzi dvoma susednými zariadeniami. Rovina management plane

zodpovedná za konfiguráciu zariadenia a nastavuje rovina control plane, v tomto prípade smerovanie z zariadení. Po výmene informácií so susednými smerovačmi sa vytvoria príslušné tabuľky a nakoniec smerovacia tabuľka, ktorá sa využíva pri rozhodovaní prepínania paketov v revine data plane.



Obr. 3.3: Rozdelenie rovín v smerovači, tok informácií v jeho vnútri a medzi susednými smerovačmi [9]

3.4 Riadenie a zneužitie prístup

AAA, username, accounts, enable psswd, ssh, ACL(data plane, je to data plane?) 92, 111, 112, bannery plus logovanie neuspesnych pristupov

3.5 Smerovacie protokoly

autentizacia, passive, ip source routing, urpf

3.6 Identifikácia zariadení, pravidiel a nastavení

host,domainname, acl remark, int description, vlan description

3.7 Šifrovanie hesiel

3.8 Logovanie

syslog, snmp nastavenie oboch, plus co logovat, teda accouting a logovanie deny pravidiel, 93

3.9 Synchronizácia času

ntp + amplifikacne utoky

3.10 Záloha a zabezpečenie konfigurácií

archive, tftp, scp, delete protection, logovanie zmien, mozno netreba, ak je AAA accounting

3.11 Správanie pri vysokom zaťažení

68-71, storm control

3.12 Monitorovanie výkonu siete

SPAN NETFLOW

3.13 Problémy vrstvy L2

access, max, hopping, double tagging, blackhole, default access a trunk, dtp, spanning tree, dot1x, vtp

3.14 First Hop Security

130 - 138 140 144-148 aj mac spoof a mac floof, teda spanning tree prikazy!!! http://isp-servis.com/?p=191

3.15 First Hop Redundancy Protocols

3.16 Tunely

3.17 Mapovanie siete a objavovanie zariadení

proxy arp, 88-91, lldp, cdp, 139

3.18 Nepoužívané a nebezpečné služby

3.19 Ostatné

source interfaces loopback shutdown

4 Návrh

4.1 Požiadavky na aplikáciu a existujúce riešenia

Kľúčovou vlastnosťou je modularita navrhovanej aplikácie, vďaka ktorej bude možné pridávať a definovať nové moduly na základe zmien v syntaxi a sémantike príkazov. Modularita taktiež umožňuje vytvorenie a podporu ďalších výrobcov a operačných systémov sieťových zariadení. Existujúce riešenia sú zväčša zamerané iba na jedného výrobcu a operačný systém, pričom program je jeden zdrojový súbor, ktorý bez dobrej znalosti kódu je problematické upraviť a rozšíriť. Preto jednotlivé overovania odporúčaní a ich následná oprava bude každé v separátnom module, ktorý budú musieť dodržať určité vstupy a výstupy, teda akési *Application programming interface* (API). Existujúce riešenia nedisponujú žiadnym generovaním opravnej konfigurácie na základe nálezu nedostatku, preto vzniknutá aplikácia bude podporovať aj vygenerovanie nápravy.

Príkladom open-source riešenia je `Cisco Config Analysis Tool`, ktorý čerpá odporúčania z jednej z kníh [7], pomocou ktorej boli vytvorené aj odporúčania v tejto práci. V tomto riešení však chýba veľa dôležitých prevádzkových a bezpečnostných odporúčaní z dôvodu, že námetom na kontrolný zoznam pri zostavovaní aplikácie bola iba jedna kniha. Taktiež podporuje iba jedného výrobcu sieťových zariadení a chýba mu modularita, nerozlišuje odporúčania a kontrolu ich prítomnosti na základe umiestnenia sieťového zariadenia v hierarchickom modeli. Nástrojom s podobnými vlasnosťami a nedostatkami je aj `Router Auditing Tool`, ktorý má naviac aj *graphical user interface – grafické užívateľské rozhranie* (GUI). Existuje niekoľko rozšírení aj pre nástroj `Nessus`, ktoré overujú dodržiavanie odporúčaní a podľa zistení čerpajú z CIS Benchmarku [10] prípadne z ekvivalentu benchmarku pre zariadenia od výrobcu Juniper. Taktiež však nepodporujú zjednanie nápravy a ignorujú umiestnenie zariadenia v topológii.

Výhodou výsledného programu je aj, že kontrolný zoznam vznikol z viacerých knižných odporúčaní a benchmarkov organizácií zaoberajúcimi sa danou problematikou. Program bude umožňovať spúšťanie modulov zodpovedných za nájdenie a odstránenie nedostatkov na základe definovaného umiestnenia zariadenia v hierarchickom modely siete. Tým sa zamedzí generovaniu falošne pozitívnych správ, ktoré by vznikli v dôsledku overovania nerelevantných požiadavkov na zariadenie v danej vrstve modelu. V neposlednom rade bude riešenie zdarma s možnosťou nahliadnuť a modifikovať respektíve rozšíriť kód.

4.2 Rozdelenie príkazov

Na zariadeniach od firmy Cisco s operačným systémom IOS bol vykonaný rozbor možných príkazov a ich foriem zápisu a početnosti výskytu v konfigurácií. Tento rozbor bol spravený z dôvodu, že niektoré príkazy sa môžu opakovať a zároveň jeden druh príkazu môže byť konfigurovaný v rôznych kontextoch a teda neprítomnosť v jednom kontexte automaticky neznamená nedostatok v konfigurácií. Na základe rozboru boli rozdelené príkazy na konfiguráciu sieťových zariadení do nasledujúcich štyroch kategórií:

1. Maximálne s jedným výskytom v konfigurácii – príkladom môže byť verzia protokolu SSH.

   Výpis 4.1: Konfigurácia verzie protokolu SSH

```
Router(config)#ssh version 2                                    1
```

2. Viacnásobný výskyt viazaný na rozhranie – typickým príkladom je zabezpečenie portu s definovaním maximálneho počtu povolených *Media Access Control* (MAC) adries.

   Výpis 4.2: Konfigurácia maximálneho počtu povolených MAC adries na porte

```
Router(config)#interface FastEthernet0/1                        1
Router(config-if)#switchport port-security mac address          2
   maximum 1
```

3. Viacnásobný výskyt v konfigurácii – tieto príkazy konfigurujú rôzne služby, napríklad autentizáciu správ OSPF.

   Výpis 4.3: Konfigurácia autentizácie OSPF na porte alebo v proccese

```
Router(config)#interface FastEthernet0/1                        1
Router(config-if)#ip ospf message-digest-key 1 md5 heslo        2
Router(config-if)#ip ospf authentication message-digest         3
                                                                4
Router(config)#router ospf 1                                    5
Router(config)#area 0 authentication message-digest             6
Router(config)#area 0 authentication key-chain 1                7
```

4. Všeobecný príkaz pre celé zariadenie a zároveň viacnásobný výskyt viazaný na

rozhranie – s týmto nastavením je možné sa stretnúť pri protokole *Link Layer Discovery Protocol* (LLDP), ktorý je možné zapnúť pre všetky porty globálne a následne selektovať porty, na ktorých nebude bežať.

Výpis 4.4: Konfigurácia protokolu LLDP a vypnutie protokolu pre jeden port

```
Router(config)#lldp run
Router(config)#interface FastEthernet0/1
Router(config-if)#no lldp receive
Router(config-if)#no lldp transmit
```

4.3 Rozdelenie sieťových prvkov

Sieť je dnes navrhovaná zväčša podľa hierarchického modelu opísaného v kapitole 3.1. Preto sa aj problémy a útoky v návrhu zatrieďujú podľa vrstvy, ktorú ovplyvňujú. V praxi sa však v menších sieťach funkcie jednotlivých vrstiev zlučujú, a preto boli okrem štandardných vrstiev nad rámec hierarchického modelu definované nasledujúce:

- CORE/EDGE – core vrstva, prípadne s funkciou hraničného prvku.
- DIST – distribučná vrstva.
- ACC – prístupová vrstva.
- COLALL – všetky vyššie zmienené vrstvy zlúčené do jednej.
- COLDISTACC – zlúčená distribučná a prístupová vrstva.
- COLCOREDIST – zlúčená core a distribučná vrstva.

4.4 Zoznam odporúčaní

TODO: citacie k jednotlivym riadkom, prejst este raz planes a severity, eliminovat viac riadkov s loopback, skratky z tabulky treba vypisat

V súčasnej dobe existuje mnoho odporúčaní, štandardov a benchmarkov, ktoré sa zaoberajú bezpečnosťou a správnou konfiguráciou sieťových zariadení. V mnohých prípadoch sú buď príliš všeobecné a teda sieťoví inžinieri majú problém zistiť, čo daným odporúčaním autor myslel a ako ho implementovať, alebo sú určené iba pre zariadenia od jedného výrobcu. Problémom je taktiež, že väčšina odporúčaní, štandardov a benchmarkov sa nie úplne prekrývajú, a teda je potrebné pri nastavovaní a audite zariadení čerpať s mnohých naraz. Výsledná tabuľka obsahuje odporúčania z odbornej literatúry a štandardov a benchmarkov verejne dostupných a používaných v produkčnom nasadení. Výhodou je aj fakt, že obsahuje odporúčania vychádzajúce

z problémov IPv6, ktoré nie sú často v štandardoch a benchmarkoch dostupné. Podrobná tabuľka s mapovaním odporúčaní na príkazy pre zariadenia Cisco s operačným systémom IOS je v prílohe TODO priloha

Zariadenia Cisco boli pre túto prácu vybrané z dôvodu, že spoločnosť Cisco je lídrom ktorý udáva trend, ich zariadenia sú celosvetovo v korporáciách veľmi rozšírené a mnoho literatúry a benchmarkov sa odvoláva na nastavenia týchto prístrojov s udávanými príkladmi konfigurácie. Taktiež sú tieto zariadenia dobrým referenčným príkladom pre hľadanie alternatívy v zariadeniach od iných výrobcov.

V tabuľke 4.1 je možné vidieť, že odporúčania sú rozdelené podľa viacerých kritérií. V prvom rade sú to roviny (plane), ktoré nie sú dôležité pre následnú automatickú konfiguráciu a odhaľovanie problémov, ale na vytvorenie si obrazu, ktorá časť rovín je kritická a postihnuteľná najviac.

Stĺpec závažnosť (severity) vznikol odhadom na základe znalostí a skúseností. Tento atribút bude možné zmeniť v konfiguračnom súbore každého modulu v závislosti na riziku, ktoré sa pre danú topológiu a firmu vyhodnotí za pomoci manažmentu rizík opísaného v kapitole 2. Tento atribút sa nenachádza v žiadnom štandarde ani benchmarku, z ktorého vytvorený zoznam odporúčaní čerpal, no je veľmi dôležitý z hľadiska, že nie všetky nedostatky sú rovnako závažné a nemajú rovnaký dopad. Hodnoty, ktoré nadobúda sú prebrané zo štandardu CVSS, pričom posledný interval `none` reprezentujúci nulové riziko respektíve závažnosť je zamenený za kľúčové slovo `notify`. K tejto zmene prišlo z dôvodu, že problémy s nulovým rizikom nie sú súčasťou návrhu a nemá zmysel ich riešiť. V prípade, že bude nález falošne pozitívny alebo riziko bude akceptované, tak sa táto skutočnosť uloží do konfiguračného súboru. Závažnosť `notify` bude použitá v prípade prítomnosti monitorovania portu pomocou zrkadlenia portu alebo NetFlow/sFlow. Jedná sa totiž o technológie potrebné na monitorovanie prevádzky z legislatívnych alebo bezpečnostných dôvodov. Riziko existuje iba pri nesprávnom nastavení zdrojov monitorovania a cieľu pre zber dát, a preto je dobré vedieť pri audite o prítomnosti tohto nastavenia.

Ďalším atribútom tabuľky je stĺpec zariadenie (facility), ktorý rozlišuje ktorých zariadení sa problém alebo útok týka. Zariadenia sú rozdelené na smerovač (R), prepínač (L2SW) a L3 prepínač (L3SW). Rozdelenie na prvky z L2 a L3 vrstvy môže byť vykonané automaticky na základe rozpoznania v konfigurácií.

Posledným rozdelením je vrstva, na ktorej zariadenie pracuje (facility layer), nakoľko rozdelenie podľa zariadení nie je dostatočné, pretože napríklad L3 prepínač môže byť použitý na ktorejkoľvek vrstve hierarchického modelu a každá vrstva má určité špecifiká, ktoré neobsahuje iná vrstva. Každý konfiguračný súbor popisujúci zariadenie bude obsahovať informáciu, do ktorej vrstvy patrí a na základe toho bude môcť program rozhodnúť, ktoré moduly zodpovedné za nájdenie problému a jeho vyriešenie budú na zariadení spustené. Taktiež bude možné meniť, dopĺňať a

zakázať spúšťanie modulov pre jednotlivé zariadenia, pokiaľ by v danej topológii nevyhovovalo rozdelenie z tabuľky 4.1.

Vrstva, na ktorej zariadenie operuje, ako aj definované zariadenie, ktorého sa odporúčanie a opatrenie týka nie sú súčasťou žiadneho kontrolného zoznamu, benchmarku ani štandardu, z ktorého bolo čerpané. Sieťový administrátor preto musí sám vyvodiť záver, ktoré odporúčania a postupy bude aplikovať na jednotlivé zariadenia a vrstvy hierarchického modelu. Preto vytvorená tabuľka odporúčaní už obsahuje aj zoznam zariadení, ktorých sa opatrenie týka.

Útok / Problém	Mitigácia / Konfigurácia typu "Best practise"	Plane [DATA| CONTROL| MANAGEMENT]	Severity [CRITICAL| HIGH| MEDIUM| LOW| NOTIFY][3]	Facility [R| L3SW| L2SW]	Facility layer [ACC| DIST| CORE/EDGE| COLALL| COLDISTACC| COLCOREDIST]
Nepovolený prístup k manažovaniu zariadenia	Vytvoriť a aplikovať ACL pre OOB, Telnet, SSH a pod. a zaznamenať v logu prístupy	Management	CRITICAL	VŠETKY	VŠETKY
Nemožná identifikácia zariadenia	Vytvoriť hostname	Management	LOW	VŠETKY	VŠETKY
Nemožnosť vzdialeného prístupu	Vytvoriť doménové meno	Management	LOW	VŠETKY	VŠETKY
Neautorizovaný prístup cez nepoužívané a nezabezpečené protokoly na manažment zariadení	Vypnúť nepoužívané protokoly na prístup k manažovaniu zariadení (telnet a pod.)	Management	HIGH	VŠETKY	VŠETKY
Prítup bez požadovaných prístupových údajov	Nakonfigruovanie protokolov na manažment zariadení, aby požadovali prístupové údaje (telnet a pod.)	Management	CRITICAL	VŠETKY	VŠETKY
Nepoužívanie zabezpečeného protokolu na manažment zariadení môže viesť k odposluchu	Zapnutie SSH	Management	CRITICAL	VŠETKY	VŠETKY
Nebezpečná verzia 1 protokolu SSH	SSH verzia 2	Management	CRITICAL	VŠETKY	VŠETKY
Útok na krátky RSA kĺúč	Dĺžka RSA kľúča minimálne 2048 bitov	Management	CRITICAL	VŠETKY	VŠETKY

Útok / Problém	Mitigácia / Konfigurácia typu "Best practise"	Plane [DATA| CONTROL| MANAGEMENT]	Severity [CRITICAL| HIGH| MEDIUM| LOW| NOTIFY][3]	Facility [R| L3SW| L2SW]	Facility layer [ACC| DIST| CORE/EDGE| COLALL| COLDISTACC| COLCOREDIST]
Dlhé neaktívne sedenie môže byť zneužité alebo aj fyzický prístup útočníka k aktívnemu sedeniu môže viesť k zmene konfigurácie	SSH čas vypršania sedenia	Management	MEDIUM	VŠETKY	VŠETKY
Hádanie hesla k RSA kľúču	SSH maximálny počet neúspešných pokusov	Management	HIGH	VŠETKY	VŠETKY
Útok hrubou silou na zistenie prihlasovacích údajov	Špecifikovať čas po ktorý nie je možné po N pokusoch sa prihlásiť	Management	HIGH	VŠETKY	VŠETKY
Prihlásenie na zariadenie nie je možné kvôli zablokovaniu pre príliš veľa neúspešných pokusov	Povolenie prístupu administrátorovi na základe IP adresy, keď je protokol na manažovanie zariadení nedostupný kvôli DOS útoku	Management	MEDIUM	VŠETKY	VŠETKY
Dlhé neaktívne sedenie môže byť zneužité alebo aj fyzický prístup útočníka k aktívnneum sedeniu môže viesť k zmene konfigurácie	Čas vypršania sedenia pre protokol na manažovanie zariadení	Management	MEDIUM	VŠETKY	VŠETKY
Možné prihlásenie do zariadenia cez telnet keď je prítomné SSH	Zakázať telnet ak je SSH aktívne	Management	CRITICAL	VŠETKY	VŠETKY
Útočník nie je informovaný o právnych následkoch	Právne upozornenie pri prístupe k zariadeniu	Management	LOW	VŠETKY	VŠETKY
Možnosť prečítať heslá z uniknutých konfigurácií	Zašifrovanie hesiel v otvorenej podobe	Management	CRITICAL	VŠETKY	VŠETKY
Nepovolená zmena konfigurácie zariadenia	Vytvorenie hesla na editovanie konfigurácie zariadenia	Management	CRITICAL	VŠETKY	VŠETKY
Nepovolený prístup k manažmentu konfigurácie zariadenia	Lokálne zabezpečené účty	Management	CRITICAL	VŠETKY	VŠETKY

Útok / Problém	Mitigácia / Konfigurácia typu "Best practise"	Plane [DATA| CONTROL| MANAGEMENT]	Severity [CRITICAL| HIGH| MEDIUM| LOW| NOTIFY][3]	Facility [R| L3SW| L2SW]	Facility layer [ACC| DIST| CORE/EDGE| COLALL| COLDISTACC| COLCOREDIST]
Centrálna správa prihlásení a dohľadateľnosť zmien v konfigurácií	Definovanie a povolenie AAA serveru na prihlásenie a definovanie záložného prihlásenia	Management	HIGH	VŠETKY	VŠETKY
Centrálna správa prihlásení a dohľadateľnosť zmien v konfigurácií	Definovanie a povolenie AAA serveru na editáciu konfigurácií a definovanie záložného prihlásenia	Management	MEDIUM	VŠETKY	VŠETKY
Hádanie prístupových údajov	Definovanie maximálneho počtu neúspešných pokusov o prihlásenie a následné zablokovanie účtu	Management	HIGH	VŠETKY	VŠETKY
Prihlásenie bez prihlasovacích údajov	Zakázať záložné prihlásenie bez poskynutia autentizačných prostriedkov	Management	CRITICAL	VŠETKY	VŠETKY
AAA používa primárne lokálne účty namiesto centralizovaných na serveri	AAA nesmie používať ako prvú možnosť prihlásenia lokálny účet	Management	HIGH	VŠETKY	VŠETKY
Používateľ prihlásený do zariadenia môže spúšťať akékoľvek príkazy	Nastavenie AAA autorizácie pre spúštanie príkazov. V prípade výpadku AAA serveru, bude užívateľ odhlásený a následne prihlásený podľa záložného prihlásenia, aby mu nebolo pridelené vysoké oprávnenie umožňujúce vykonávať príkazy, na ktoré nemá právo	Management	HIGH	VŠETKY	VŠETKY
Administrátor vloží zlý príkaz a po čase je ho nemožné dohľadať a zjednať nápravu	Nastavenie AAA účtovania respektíve logovania pripojení a vykonaných príkazov	Management	HIGH	VŠETKY	VŠETKY
AAA zdrojové rozhranie nie je rovnaké pri každom reštarte	Definovanie loopback zdrojového rozhrania pre AAA	Management	MEDIUM	VŠETKY	VŠETKY
Odpočúvanie SNMP verzie 1 a 2c	Použitie SNMP verie 3 pokiaľ je SNMP používané	Management	CRITICAL	VŠETKY	VŠETKY

Útok / Problém	Mitigácia / Konfigurácia typu "Best practise"	Plane [DATA| CONTROL| MANAGEMENT]	Severity [CRITICAL| HIGH| MEDIUM| LOW| NOTIFY][3]	Facility [R| L3SW| L2SW]	Facility layer [ACC| DIST| CORE/EDGE| COLALL| COLDISTACC| COLCOREDIST]
Modifikovanie konffigurácie pomocou SNMP	Obmedzenie SNMP iba na čítanie	Management	CRITICAL	VŠETKY	VŠETKY
Neoprávnený prístup k SNMP informáciám	Obmedzenie SNMP iba pre vybrané IP adresy	Management	HIGH	VŠETKY	VŠETKY
Administrátor nemá povedomie o problémoch na zariadení	Povolenie asynchrónnych správ SNMP TRAP	Management	MEDIUM	VŠETKY	VŠETKY
Odpočúvanie SNMP sedenie z dôvodu slabého šifrovania a hashovacej funkcie	Vytvorenie SNMP verzie 3 užívateľa s minimálnym šifrovaním AES 128 bit a hashovacou funkciou SHA	Management	CRITICAL	VŠETKY	VŠETKY
Sťažená identifikácia SNMP správ z rôznych IP	Definovanie lokácie SNMP serveru	Management	LOW	VŠETKY	VŠETKY
SNMP zdrojové rozhranie nie je rovnaké pri každom reštarte	Definovanie loopback zdrojového rozhrania pre SNMP	Management	MEDIUM	VŠETKY	VŠETKY
Zmeny názvov rozhraní medzi reštartami a nemožnosť monitorovanie pomocou SNMP	SNMP statické nemenné meno rozhrania aj po reštarte zariadenia	Management	HIGH	VŠETKY	VŠETKY
Administrátor nemá povedomie o problémoch na zariadení	Povolenie logovania protokolom SYSLOG a špecifikovanie IP adresy SYSLOG serveru	Management	HIGH	VŠETKY	VŠETKY
Neprijímanie všetkých dôležitých incidentov na zariadení z protokolu SYSLOG	Špecifikovanie dôležitosti oznámení SYSLOG na INFORMATIONAL	Management	MEDIUM	VŠETKY	VŠETKY
SYSLOG zdrojové rozhranie nie je rovnaké pri každom reštarte	Definovanie loopback zdrojového rozhrania pre SYSLOG	Management	MEDIUM	VŠETKY	VŠETKY
Nedostatočné a neštandardné formáty času v logovacích správach	Definovanie formátu času pre logovacie a ladiace výstupy	Management	MEDIUM	VŠETKY	VŠETKY

Útok / Problém	Mitigácia / Konfigurácia typu "Best practise"	Plane [DATA| CONTROL| MANAGEMENT]	Severity [CRITICAL| HIGH| MEDIUM| LOW| NOTIFY][3]	Facility [R| L3SW| L2SW]	Facility layer [ACC| DIST| CORE/EDGE| COLALL| COLDISTACC| COLCOREDIST]
Administrátor nevidí dôležité incidenty pri prihlásení a konfigurovaní cez konzolu	Vypisovanie SYSLOG správ CRITICAL a dôležitejších do terminálu	Management	MEDIUM	VŠETKY	VŠETKY
Malá vyrovnávacia pamäť pre SYSLOG je dôvodom zahadzovanie správ	Definovanie veľkosti SYSLOG buffera dôležitosti oznámení na INFORMATIONAL	Management	HIGH	VŠETKY	VŠETKY
Neprístupný SYSLOG server spôsobuje zahadzovanie dôležitých syslog správ	Definovanie dočasného úložiska SYSLOG správ v prípade nedostupnosti servera	Management	HIGH	VŠETKY	VŠETKY
Skenovanie a zistenie informácií o sieti za pomoci protokolu CDP a využitie bezpečnostných chýb	Zakázanie protokolu CDP	Management	CRITICAL	VŠETKY	VŠETKY
Skenovanie a zistenie informácií o sieti za pomoci protokolu LLDP a využitie bezpečnostných chýb	Zakázanie protokolu LLDP	Management	CRITICAL	VŠETKY	VŠETKY
Nekonzistencia časov v logoch a problém pričlenenia logov k relevantným incidentom	Nastavenie NTP serveru pre aktuálny čas v logoch	Management	HIGH	VŠETKY	VŠETKY
Pripojenie servera s rovnakou IP adresou, ale falošným časom	Nastavenie NTP autentizácie	Management	HIGH	VŠETKY	VŠETKY
NTP zdrojové rozhranie nie je rovnaké pri každom reštarte	Definovanie loopback zdrojového rozhrania pre NTP	Management	MEDIUM	VŠETKY	VŠETKY
Väčšia bezpečnosť (pub/priv key) NTP a podpora IPv6	Použitie NTP verzie 4	Management	MEDIUM	VŠETKY	VŠETKY

Útok / Problém	Mitigácia / Konfigurácia typu “Best practise”	Plane [DATA| CONTROL| MANAGEMENT]	Severity [CRITICAL| HIGH| MEDIUM| LOW| NOTIFY][3]	Facility [R| L3SW| L2SW]	Facility layer [ACC| DIST| CORE/EDGE| COLALL| COLDISTACC| COLCOREDIST]
Falošný čas od podvrhnutého NTP zdroja	Nastavenie NTP peer s inými sieťovými zariadeniami na krížovú validáciu času a záložný zdroj času	Management	MEDIUM	VŠETKY	VŠETKY
Útočník s fyzickým prístupom k zariadeniu alebo portu môže odpočúvať alebo posielať škodlivý obsah	Explicitne zakázať nepoužívané porty	Data	CRITICAL	VŠETKY	VŠETKY
Zdrojové rozhranie pre management a control protokoly	Vytvoriť Loopback rozhranie s IP adresou	Control	MEDIUM	VŠETKY	VŠETKY
Identifikácia pravidla v ACL	Popis každého pravidla v ACL pre lepšiu identifikáciu	Management	LOW	VŠETKY	VŠETKY
Indentifikácia rozhrania	Popis každého rozhrania	Management	LOW	VŠETKY	VŠETKY
SSH zdrojové rozhranie nie je rovnaké pri každom reštarte	Definovanie loopback zdrojového rozhrania pre SSH	Management	MEDIUM	VŠETKY	VŠETKY
DOS útok na štandardný SSH port 22	Špecifikovanie iného portu pre SSH ako štandardného alebo aplikovanie port knocking	Management	HIGH	VŠETKY	VŠETKY
Nepovolený prístup k manažmentu konfigurácie zariadenia	Vypnutie odchádzajúcich spojení pre protokoly na manažment zariadení pokiaľ sa nepoužívajú (telnet a pod.)	Management	HIGH	VŠETKY	VŠETKY
Odpočuvanie konfigurácií zariadení pri zálohe	Zapnutie zabezpečenej zálohy na server (SFTP, SCP)	Management	HIGH	VŠETKY	VŠETKY
Vymazanie konfigurácie	Zapnutie ochrany pred výmazom konfigurácie	Management	HIGH	VŠETKY	VŠETKY
Možnosť urobiť diff zmien konfigurácií a jej návrat	Periodické zálohovanie konfigurácie a logovanie jej zmien	Management	MEDIUM	VŠETKY	VŠETKY
DOS útok alebo pokus o prístup k tomu, čo nie je povolené	Logovanie pravidiel zahodenia paketov v ACL	Management	MEDIUM	VŠETKY	VŠETKY

Útok / Problém	Mitigácia / Konfigurácia typu "Best practise"	Plane [DATA| CONTROL| MANAGEMENT]	Severity [CRITICAL| HIGH| MEDIUM| LOW| NOTIFY][3]	Facility [R| L3SW| L2SW]	Facility layer [ACC| DIST| CORE/EDGE| COLALL| COLDISTACC| COLCOREDIST]
Nízky stav voľnej pamäte	Nastavenie notifikácie pri dochádzaní pamäte	Management	MEDIUM	VŠETKY	VŠETKY
Logovacie správy nemôžu byť zaznamenané kvôli nedostatku pamäte	Rezervovanie pamäte pre kritické notifikácie pri nedostatku pamäte	Management	HIGH	VŠETKY	VŠETKY
Vysoké zaťaženie CPU	Nastavenie notifikácie vysokom zaťažení CPU	Management	MEDIUM	VŠETKY	VŠETKY
Vysoké zaťaženie zariadenia spôsobilo nemožnosť prihlásenia k nemu	Rezervovanie pamäte preprotokoly na manažment zariadení pri nedostatku pamäte	Management	HIGH	VŠETKY	VŠETKY
Pretečenie pamäte	Povoliť mechanizmy na detekciu pretečenia pamäte	Management	MEDIUM	VŠETKY	VŠETKY
Načítanie škodlivej konfigurácie zo siete počas bootovania	Vypnutie načítania operačného systému alebo konfigurácie zo siete pokiaľ to nie je nutné	Management	MEDIUM	VŠETKY	VŠETKY
Proxy ARP môže viesť k obídeniu PVLAN a rozširuje broadcast doménu	Vypnutie Proxy ARP	Control	CRITICAL	R, L3SW	CORE/EDGE, DIST, COLCOREDIST, COLDISTACC, COLALL
DOS útok na stanicu, cez ktorú bola špecifikovaná cesta a teda nemožnosť komunikácie s koncovým bodom. Alebo zosnovanie MITM útoku	Vypnutie IP source routing	Control	CRITICAL	R, L3SW	CORE/EDGE, DIST, COLCOREDIST, COLDISTACC, COLALL
DOS útok pomocou podvrhnutej IP adresy alebo vzdialený útok na smerovací protokol	Zapnutie reverse path forwarding strict/loose mode	Control	HIGH	R, L3SW	CORE/EDGE, DIST, COLCOREDIST, COLDISTACC, COLALL
Nepoužívané, staré a nezabezpečené služby môžu byť použité na škodlivé účely	Vypnutie nepoužívaných služieb z bezpečnostných dôvodov a na šetrenie CPU a pamäte	Záleží na výrobcovi a zariadení	HIGH	Záleží na výrobcovi a zariadení	Záleží na výrobcovi a zariadení

Útok / Problém	Mitigácia / Konfigurácia typu "Best practise"	Plane [DATA| CONTROL| MANAGEMENT]	Severity [CRITICAL| HIGH| MEDIUM| LOW| NOTIFY][3]	Facility [R| L3SW| L2SW]	Facility layer [ACC| DIST| CORE/EDGE| COLALL| COLDISTACC| COLCOREDIST]
Útočník môže zistiť, že IP adresa, na ktorú skušal ping je nesprávna	Vypnutie spáv ICMP Unreachable	Data	HIGH	R, L3SW	CORE/EDGE, DIST, COLCOREDIST, COLDISTACC, COLALL
Útočník môže zistiť masku podsiete pomocou ICMP Mask reply	Vypnutie spáv ICMP Mask reply	Data	HIGH	R, L3SW	CORE/EDGE, DIST, COLCOREDIST, COLDISTACC, COLALL
Umožňuje DOS Smurf útok, mapovanie siete pomocou ping na broadcast adresu vzdialenej siete	Vypnutie ICMP echo správ na broadcast adresu, vypnutie directed broadcasts	Data	CRITICAL	R, L3SW	CORE/EDGE, DIST, COLCOREDIST, COLDISTACC, COLALL
Útočník môže zistiť smerovacie informácie alebo vyťažiť CPU	Vypnutie spáv ICMP Redirects	Data	HIGH	R, L3SW	CORE/EDGE, DIST, COLCOREDIST, COLDISTACC, COLALL
Nekonzistenia konfiguračných súborov pri zmenách konfigurácie viac ako jedným administrátorom	Povolit súčasne iba jednému administrátorovi vykonávanie zmien v konfigurácii	Management	HIGH	VŠETKY	VŠETKY
Problém identifikácie SYSLOG správ s rovnakou časovou značkou	Pridanie sekvenčného čísla ku každej syslog správe	Management	LOW	VŠETKY	VŠETKY
Nemožnosť prihlásenia pri zaseknutom TCP spojení	Terminovanie zaseknutého TCP spojenia	Management	MEDIUM	VŠETKY	VŠETKY
Vloženie a manipulácia so smerovacími informáciami	Autentizácia smerovacích protokolov (nie heslá v otvorenej podobe)	Control	HIGH	R, L3SW	CORE/EDGE, DIST, COLCOREDIST, COLDISTACC, COLALL
OSPF virtuálne linky degradujú výkon	Vypnutie virtuálnych liniek pre OSPF	Control	HIGH	R, L3SW	CORE/EDGE, DIST, COLCOREDIST, COLDISTACC, COLALL
Koncové zariadenie, užívateľ a útočník môžu vidiet smerovacie správy a topológiu siete alebo pripojenie škodlivého zariadenia, ktoré vysielať a prijímať smerovacie správy	Špecifikovanie rozhraní, ktoré nebudú prijímať routovacie informácie	Control	HIGH	R, L3SW	CORE/EDGE, DIST, COLCOREDIST, COLDISTACC, COLALL

Útok / Problém	Mitigácia / Konfigurácia typu "Best practise"	Plane [DATA| CONTROL| MANAGEMENT]	Severity [CRITICAL| HIGH| MEDIUM| LOW| NOTIFY][3]	Facility [R| L3SW| L2SW]	Facility layer [ACC| DIST| CORE/EDGE| COLALL| COLDISTACC| COLCOREDIST]
Nemožnosť sprevádzkovať procesy smerovacích protokolov v určitých prípadoch pri použití IPv6	Špecifikovanie identifikátorov smerovacích protokolov pre každý router (router ID)	Control	MEDIUM	R, L3SW	CORE/EDGE, DIST, COLCOREDIST, COLDISTACC, COLALL
Vysledovateľnosť nefunkčnosti routovacieho protokolu a nesprávneho nastavenia	Zaznamenie zmeny v logu pri zmenách v smerovaní	Control	MEDIUM	R, L3SW	CORE/EDGE, DIST, COLCOREDIST, COLDISTACC, COLALL
Škodlivé vloženie smerovacích informácií informácií, vzdialený útok	TTL security	Control	HIGH	R, L3SW	CORE/EDGE, DIST, COLCOREDIST, COLDISTACC, COLALL
Nesprávne smerovanie kvôli sumarizácií	Vypnutie automatickej sumarizácie smerovacích protokolov	Control	HIGH	R, L3SW	CORE/EDGE, DIST, COLCOREDIST, COLDISTACC, COLALL
Packety budú spracovávané v CPU, ktoré môže byť preťažené a môže byť zmenené smerovanie na obídenie bezpečnostnej kontroly	Zahadzovanie IPv4 paketov s rozšírenou hlavičkou (IP Options filtering)	Control	CRITICAL	R, L3SW	CORE/EDGE, DIST, COLCOREDIST, COLDISTACC, COLALL
Odpočúvanie komunikácie cez nezabezpečené tunely	Vypnúť tunely ktoré nie sú zabezpečené alebo zabezpečiť tunely	Data	CRITICAL	R, L3SW	CORE/EDGE, DIST, COLCOREDIST, COLDISTACC, COLALL
Môže byť zneužité odpočúvanie pokiaľ sa používa monitorovanie prevádzky a monitorovanie prevádzky kvôli legislatívnym potrebám	Monitorovanie výkonnosti siete a zber sieťového prenosu kvôli legislatívnym potrebám	Control	NOTICE	VŠETKY	VŠETKY
IP spoofing	Špecifikácia ACL na zakázanie a logovanie privátnych a špeciálnych IP adries z RFC 1918, RFC 3330	Control	CRITICAL	R, L3SW	CORE/EDGE, COLCOREDIST, COLALL
IP spoofing	Špecifikácia ACL na zakázanie a logovanie špeciálnych IPv6 adries z RFC 5156	Control	CRITICAL	R, L3SW	CORE/EDGE, COLCOREDIST, COLALL

Útok / Problém	Mitigácia / Konfigurácia typu "Best practise"	Plane [DATA| CONTROL| MANAGEMENT]	Severity [CRITICAL| HIGH| MEDIUM| LOW| NOTIFY][3]	Facility [R| L3SW| L2SW]	Facility layer [ACC| DIST| CORE/EDGE| COLALL| COLDISTACC| COLCOREDIST]
Rogue root bridge	Rogue root bridge protection (root guard)	Control	CRITICAL	L3SW, L2SW	DIST, COLDISTACC, ACC
Pripojenie prepínaču na koncový prístupový port	BPDU protection (BPDU guard)	Control	CRITICAL	L3SW, L2SW	DIST, COLDISTACC, ACC
Rýchlosť konvergencie	Prístupové porty by sa nemali podielať na STP procese	Control	HIGH	L3SW, L2SW	DIST, COLDISTACC, ACC
Unidirectional communication between switches can lead to loop topology/ Jednosmerná komunikácia medzi prepínačmi môže viesť k topoógií so slučkami	Špeciálne konfigurácie zaisťujúce bezslučkovú topológiu pomocou STP keď nastane jednosmerná komunikácia (Loop Guard)	Control	CRITICAL	L3SW, L2SW	DIST, COLDISTACC, ACC
Nemožnosť identifikácie účelu VLAN	Pridanie mena k VLAN	Control	LOW	L3SW, L2SW	DIST, COLDISTACC, ACC
Špeciálna VLAN pre manažment na obmedzenie prístupu iba pre administrátorov	Vytvorenie separátnej VLAN pre manažment	Control	MEDIUM	L3SW, L2SW	DIST, COLDISTACC, ACC
Útočníkovi s fyzickým prístupom k portu môže byť pridelený prístup do časti siete, ktorá zodpovedá príslušnej VLAN	Vytvorenie špeciálnej black hole VLAN pre nevyužité porty	Control	CRITICAL	L3SW, L2SW	DIST, COLDISTACC, ACC
Predvolenej VLAN je povolené prepnute na akýkoľvek port, VLAN hopping, double tagging	Odobrať všetky porty z predvolenej VLAN	Control	CRITICAL	L3SW, L2SW	DIST, COLDISTACC, ACC
Predvolenej VLAN je povolené byť prepnutá na akýkoľvek port, VLAN hopping, double tagging	Vytvorenie natívnej VLAN rozdielnej ako predvolená, priradeni k trunk portu a povolenie iba potrebných portov	Control	CRITICAL	L3SW, L2SW	DIST, COLDISTACC, ACC

Útok / Problém	Mitigácia / Konfigurácia typu "Best practise"	Plane [DATA| CONTROL| MANAGEMENT]	Severity [CRITICAL| HIGH| MEDIUM| LOW| NOTIFY][3]	Facility [R| L3SW| L2SW]	Facility layer [ACC| DIST| CORE/EDGE| COLALL| COLDISTACC| COLCOREDIST]
DTP útok, Switch spoofing útok	Vypnutie dynamického trunkovacieho protokolu a explicitne určiť porty ako prístupové a trunk	Control	CRITICAL	L3SW, L2SW	DIST, COLDISTACC, ACC
MAC Spoofing, MAC Flooding	Definovanie maximálne 1 MAC adresy na port, priradenie MAC adresy na port	Control	CRITICAL	L3SW, L2SW	DIST, COLDISTACC, ACC
MAC Spoofing, MAC Flooding	Nastavenie režimu narušenia, ktorý vypne port alebo informuje správcu o pripojení nepovoleného zariadenia	Control	HIGH	L3SW, L2SW	DIST, COLDISTACC, ACC
Nový prepínač s vyšším číslom revízie, ale s nesprávnou VLAN databázou môže šíriť falošné VLAN identifikátory a spôsobiť nefunkčnosť siete, veľa možnch VTP útokov kvôli zraniteľnostiam	Vypnutie MVRP. MRP, GARP, VTP po úspešnej propagácií VLAN	Control	CRITICAL	L3SW, L2SW	DIST, COLDISTACC, ACC
VTP musí byť používané	Use VTP v3 with set password and enable VTP prunning when VTP must be enabled/ Uprednostniť VTP verzie 3, špecifikovať skryté heslo a zapnúť VTP prunning pokiaľ musí byť VTP zapnuté	Control	CRITICAL	L3SW, L2SW	DIST, COLDISTACC, ACC
Vysoké zaťaženie linky	Poslanie notifikácie pri prekročení prahovej hodnoty zaťaženia linky	Control	MEDIUM	VŠETKY	VŠETKY
Využívanie siete nepovolenými používateľmi	Zapnutie 802.1x	Control	HIGH	L3SW, L2SW	DIST, COLDISTACC, ACC
Útok hrubou silou hádaním prístupových údajov pre 802.1x	Limitovanie maximálneho počtu neúspešných pokusov o autentizáciu 802.1x	Control	HIGH	L3SW, L2SW	DIST, COLDISTACC, ACC

Útok / Problém	Mitigácia / Konfigurácia typu "Best practise"	Plane [DATA| CONTROL| MANAGEMENT]	Severity [CRITICAL| HIGH| MEDIUM| LOW| NOTIFY][3]	Facility [R| L3SW| L2SW]	Facility layer [ACC| DIST| CORE/EDGE| COLALL| COLDISTACC| COLCOREDIST]
IPv6 ND Spoofing	IPv6 ND Inspection	Control	CRITICAL	L3SW, L2SW	DIST, COLDISTACC, ACC
Rogue RARA FloodRoute Information Option injectionRA RouterLifeTime=0	RA Guard	Control	CRITICAL	L3SW, L2SW	DIST, COLDISTACC, ACC
DHCP spoofing	DHCP snooping, IPv6 Snooping, DHCPv6 Guard	Control	CRITICAL	L3SW, L2SW	DIST, COLDISTACC, ACC
Příliš veľa DHCP paketov, zaplavenie DHCP paketmi	Odmedziť počet DHCP paketov na nedôverihodných rozhraniach	Control	MEDIUM	L3SW, L2SW	DIST, COLDISTACC, ACC
ARP Spoofing	Dynamic ARP Inspection	Control	CRITICAL	L3SW, L2SW	DIST, COLDISTACC, ACC
IP spoofing	IPv4/IPv6 Source Guard	Control	CRITICAL	L3SW, L2SW	DIST, COLDISTACC, ACC
IPv6 Next Header a IPv6 Fragmentation útok	ACL blokujúce nerozpoznateľne rozšírené hlavičky	Control	CRITICAL	VŠETKY	VŠETKY
Mapovanie sete pomocou pingu na multicast adresu všetkých uzlov a MLD Query Overload a Smurf útok	ACL blokujúce ICMP echo request na multicast adresu všetkých uzlov a MLD Query na prístupových portoch	Control	MEDIUM	L3SW, L2SW	DIST, COLDISTACC, ACC
Mobilné zariadenia pripojené bezdôtovo spotrebovávajú veľa energie kvôli častým RA správam	RA Throttling	Control	LOW	L3SW, L2SW	DIST, COLDISTACC, ACC
Zlyhanie zariadenia alebo linky môže viest k nefunkčnosti siete	Povolenie FHRP s autentizáciou a aktuálnou verziou	Control	MEDIUM	R, L3SW	CORE/EDGE, COLCOREDIST, COLALL
Vyčerpanie cache susedov	Statický záznam pre kritické zariadenia (servery) spájajúce IP a MAC adresu a VLAN	Control	CRITICAL	L3SW, L2SW	DIST, COLDISTACC, ACC

Útok / Problém	Mitigácia / Konfigurácia typu "Best practise"	Plane [DATA| CONTROL| MANAGEMENT]	Severity [CRITICAL| HIGH| MEDIUM| LOW| NOTIFY][3]	Facility [R| L3SW| L2SW]	Facility layer [ACC| DIST| CORE/EDGE| COLALL| COLDISTACC| COLCOREDIST]
Vyčerpanie cache susedov	Na zabránenie vzdialeného útoku na cache susedov cez internet je potreba nastaviť ACL, kde povolujeme iba komunikáciu s cieľovými IPv6 adresami, ktoré sa nachádzajú v našej sieti	Control	CRITICAL	R, L3SW	CORE/EDGE, COLCOREDIST, COLALL
Vyčerpanie cache susedov	IP destination Guard (First Hop Security)	Control	CRITICAL	L3SW, L2SW	DIST, COLDISTACC, ACC
Vyčerpanie cache susedov	Limitovanie počtu IPv6 adries v cache susedov	Control	CRITICAL	L3SW, L2SW	DIST, COLDISTACC, ACC
Vyčerpanie cache susedov	Limitovanie času IPv6 adresy v cache susedov	Control	CRITICAL	L3SW, L2SW	DIST, COLDISTACC, ACC
Vyčerpanie cache susedov	Skrátenie IPv6 prefixu, aplikovateľné iba pr použití DHCPv6	Control	CRITICAL	R, L3SW	CORE/EDGE, COLCOREDIST, COLALL
SYN Flood	Nastavenie zachytávanie firewallom pre útok flagu SYN	Control	CRITICAL	R, L3SW	CORE/EDGE, COLCOREDIST, COLALL
Komplexné bezpečnostné hrozby a narušenie bezpečnosti	Nastavenie IDS/IPS	Control	HIGH	R, L3SW	CORE/EDGE, COLCOREDIST, COLALL

Tab. 4.1: Zoznam bezpečnostných a prevádzkových problémov a odporúčaní

4.5 Hierarchická štruktúra

Stromová štruktúra a koncept fungovania, Možno fungovanie cez nejaký UML diagram (sekvenčný?) alebo skôr niečo zjednodušené

5 Implementácia

5.1 Použité technológie

5.1.1 Python

niečo o pythone, výhody, prečo je vhodný a bol vybraný

5.1.2 YAML

čo je, porovnať s XML, JSON, vlastnou syntaxou, prečo je YAML vhodný

5.1.3 Regulárne výrazy

nejaký obkec okolo (krátko), prečo sú vhodné, ako budú použité

5.2 Konfiguračné súbory

možno do implmentácie, automaticke zistovaine niektorych atributov

5.2.1 Súbor popisujúci zariadenie

device.yaml

5.2.2 Súbor popisujúci modul

module.yaml false positive, akceptovanie rizika

5.3 Moduly

Záver

Zhrnutie práce.

Literatúra

[1] MILKOVICH, Devon. 13 Alarming Cyber Security Facts and Stats. In: *Cybint* [online]. 3.12.2018 [cit. 2019-11-08]. Dostupné z: https://www.cybintsolutions.com/cyber-security-facts-stats/

[2] VYNCKE, Eric a Christopher PAGGEN. *LAN switch security: What hackers know about your switches*. Indianapolis, IN: Cisco Press, 2008. ISBN :978-1-58705-256-9.

[3] MCMILLAN, Troy. *CCNA security study guide: exam 210-260*. Indianapolis, Indiana: Sybex, a Wiley Brand, 2018. ISBN 978-111-9409-939.

[4] STALLINGS, William. *Network security essentials: applications and standards*. 4th ed. Boston: Prentice Hall, 2011. ISBN 978-0-13-610805-4.

[5] JACKSON, Chris. *Network security auditing*. Indianapolis, IN: Cisco Press, 2010. Cisco Press networking technology series. ISBN 978-1-58705-352-8.

[6] Guide for Conducting Risk Assessments: NIST Special Publication 800-30. In: *NIST* [online]. 2012 [cit. 2019-11-08]. Dostupné z: https://nvlpubs.nist.g ov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf

[7] SINGH, Shashank. Cisco Guide to Harden Cisco IOS Devices. In: *Cisco* [online]. 2018 [cit. 2019-11-02]. Dostupné z: https://www.cisco.com/c/en/us/support/docs/ip/access-lists/13608-21.html

[8] LAMMLE, Todd. *CCNA: routing and switching : study guide*. Indianapolis, Indiana: SYBEX, [2013]. ISBN 978-1-118-74961-6.

[9] PEPELNJAK, Ivan. Management, Control and Data Planes in Network Devices and Systems. In: *IpSpace* [online]. 2013 [cit. 2019-11-17]. Dostupné z: https://blog.ipspace.net/2013/08/management-control-and-data-planes-in.html

[10] CIS Cisco IOS 15 Benchmark. In: *Center For Internet Security* [online]. 2015 [cit. 2019-11-02]. Dostupné z: https://www.cisecurity.org/benchmark/cisco/

[11] ALSADEH, Ahmad. Augmented SEND: Aligning Security, Privacy, and Usability. In: *RIPE NCC* [online]. 12.5.2015 [cit. 2019-11-02]. Dostupné z: https://ripe70.ripe.net/presentations/67-RIPE70-SEND.pdf

[12] PODERMAŃSKI, Tomáš a Matěj GRÉGR. Bezpečné IPv6: zkrocení zlých směrovačů. In: *ROOT.CZ* [online]. 12.2.2015 [cit. 2019-11-02]. Dostupné z: https://www.root.cz/clanky/bezpecne-ipv6-zkroceni-zlych-smerovacu/

[13] KHANDELWAL, Manjul. OSPF Security: Attacks and Defenses. In: *SANOG* [online]. 2016 [cit. 2019-11-04]. Dostupné z: https://www.sanog.org/resources/sanog28/SANOG28-Tutorial_OSPF-Security-Attacks-and-Defences-Manjul.pdf

[14] PODERMAŃSKI, Tomáš a Matěj GRÉGR. Bezpečné IPv6: když dojde keš — obrana. In: *ROOT.CZ* [online]. 19.3.2015 [cit. 2019-11-02]. Dostupné z: https://www.root.cz/clanky/bezpecne-ipv6-kdyz-dojde-kes-obrana/

[15] PODERMAŃSKI, Tomáš a Matěj GRÉGR. Bezpečné IPv6: když dojde keš. In: *ROOT.CZ* [online]. 12.3.2015 [cit. 2019-11-02]. Dostupné z: https://www.root.cz/clanky/bezpecne-ipv6-kdyz-dojde-kes/

[16] PODERMAŃSKI, Tomáš a Matěj GRÉGR. Bezpečné IPv6: trable s multicastem. In: *ROOT.CZ* [online]. 5.3.2015 [cit. 2019-11-02]. Dostupné z: https://www.root.cz/clanky/bezpecne-ipv6-trable-s-multicastem/

[17] GRÉGR, Matěj a Tomáš PODERMAŃSKI. Bezpečné IPv6: vícehlavý útočník. In: *ROOT.CZ* [online]. 26.2.2015 [cit. 2019-11-02]. Dostupné z: https://www.root.cz/clanky/bezpecne-ipv6-vicehlavy-utocnik/

[18] PODERMAŃSKI, Tomáš a Matěj GRÉGR. Bezpečné IPv6: trable s hlavičkami. In: *ROOT.CZ* [online]. 19.2.2015 [cit. 2019-11-02]. Dostupné z: https://www.root.cz/clanky/bezpecne-ipv6-trable-s-hlavickami/

[19] GRÉGR, Matěj a Tomáš PODERMAŃSKI. Bezpečné IPv6 : směrovač se hlásí. In: *ROOT.CZ* [online]. 5.2.2015 [cit. 2019-11-02]. Dostupné z: https://www.root.cz/clanky/bezpecne-ipv6-smerovac-se-hlasi/

[20] IPv6 First-Hop Security Configuration Guide. In: *Cisco* [online]. San Jose [cit. 2019-11-02]. Dostupné z: https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipv6_fhsec/configuration/15-1sg/ip6f-15-1sg-book.pdf

[21] BOUŠKA, Petr. *Cisco IOS 12 - IEEE 802.1x a pokročilejší funkce* [online]. In: . 2007 [cit. 2019-11-02]. Dostupné z: https://www.samuraj-cz.com/clanek/cisco-ios-12-ieee-802-1x-a-pokrocilejsi-funkce/

[22] MOLENAAR, René. Cisco IOS features that you should disable or restrict. In: *NetworkLessons.com* [online]. [cit. 2019-11-02]. Dostupné z: https://networklessons.com/uncategorized/cisco-ios-features-that-you-should-disable-or-restrict

[23] BOUŠKA, Petr. Cisco IOS 23 - Autentizace uživatele na switchi vůči Active Directory. In: *SAMURAJ-cz* [online]. 2009 [cit. 2019-11-02]. Dostupné z: https://www.samuraj-cz.com/clanek/cisco-ios-23-autentizace-uzivatele-na-switchi-vuci-active-directory/

[24] BARKER, Elaine a Allen ROGINSKY. Transitioning the Use of Cryptographic Algorithms and Key Lengths. In: *NIST* [online]. 2019 [cit. 2019-11-02]. Dostupné z: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-131Ar2.pdf

[25] VYNCKE, Erik. ND on wireless links and/or with sleeping nodes. In: *IETF* [online]. [cit. 2019-11-02]. Dostupné z: https://www.ietf.org/proceedings/89/slides/slides-89-v6ops-3.pdf

[26] GRAESSER, Dana. Cisco Router Hardening Step-by-Step. In: *SANS Institute* [online]. 2001 [cit. 2019-11-02]. Dostupné z: https://www.sans.org/reading-room/whitepapers/firewalls/paper/794

[27] PILIHANTO, Atik. A Complete Guide on IPv6 Attack and Defense. In: *SANS Institute* [online]. SANS Institute, 2012 [cit. 2019-11-02]. Dostupné z: https://www.sans.org/reading-room/whitepapers/detection/paper/33904

[28] REY, Enno, Antonios ATLASIS a Jayson SALAZAR. MLD Considered Harmful. In: *RIPE NCC* [online]. 2016 [cit. 2019-11-02]. Dostupné z: https://ripe72.ripe.net/presentations/74-ERNW_RIPE72_MLD_Considered_Harmful_v1_light_web.pdf

[29] VYNCKE, Erik. IPv6 First Hop Security: the IPv6 version of DHCP snooping and dynamic ARP inspection. In: *Slidde Share* [online]. 2012 [cit. 2019-11-02]. Dostupné z: https://www.slideshare.net/IKTNorge/eric-vynckelayer2-security-ipv6-norway

[30] IPv6 First-Hop Security Configuration Guide. In: *Cisco* [online]. 2012 [cit. 2019-11-02]. Dostupné z: https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipv6_fhsec/configuration/15-s/ip6f-15-s-book/ip6-snooping.html

[31] GREGR, Matej, Petr MATOUSEK, Miroslav SVEDA a Tomas PODERMANSKI. Practical IPv6 monitoring-challenges and techniques. In: *12th IFIP/IEEE International Symposium on Integrated Network Management (IM 2011) and Workshops*. IEEE, 2011, 2011, s. 650-653. DOI: 10.1109/INM.2011.5990647. ISBN 978-1-4244-9219-0. Dostupné také z: http://ieeexplore.ieee.org/document/5990647/

[32] PODERMAŃSKI, Tomáš a Matějj GRÉGR. *Deploying IPv6 - practical problems from the campus perspective* [online]. In: . [cit. 2019-11-02].

[33] MARTIN, Tim. IPv6 Sys Admin Style. In: *SlideShare* [online]. 2016 [cit. 2019-11-02]. Dostupné z: https://www.slideshare.net/tjmartin2020/ipv6-sysadmins-63071235

[34] Cisco SAFE Reference Guide. In: *CIsco* [online]. San Jose, CA, 8 Júl 2018 [cit. 2019-11-02]. Dostupné z: https://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Security/SAFE_RG/SAFE_rg.pdf

[35] SAFE Overview Guide: Threats, Capabilities, and the Security Reference Architecture. In: *Cisco* [online]. Január 2018 [cit. 2019-11-02]. Dostupné z: https://www.cisco.com/c/dam/en/us/solutions/collateral/enterprise/design-zone-security/safe-overview-guide.pdf

[36] AKIN, Thomas. *Hardening Cisco routers*. Sebastopol: O'Reilly, 2002. ISBN 05-960-0166-5.

[37] HUCABY, Dave, Steve MCQUERRY, Andrew WHITAKER a Dave HUCABY. *Cisco router configuration handbook*. 2nd ed. Indianapolis, IN: Cisco Press, 2010. ISBN 978-1-58714-116-4.

[38] SATRAPA, Pavel. *IPv6: internetový protokol verze 6*. 4. aktualizované a rozšířené vydání. Praha: CZ.NIC, z.s.p.o., 2019. CZ.NIC. ISBN 978-808-8168-430.

Zoznam symbolov, veličín a skratiek

CIA	confidentiality, integrity, availability – dôvernosť, integrita, dostupnosť
DDoS	Distributed Denial of Service – distribuované odoprenie služby
DoS	Denial of Service – odoprenie služby
ACL	Access Control List – zoznam pre riadenie prístupu
CVSS	Common Vulnerability Scoring System
IDS	Intrusion Detection System – systém detekcie narušenia
IPS	Intrusion Prevention System – systém prevencie prienikov
FHRP	First Hop Redundancy Protocol
SNMP	Simple Network Management Protocol
AAA	Authentication Authorization Accounting
SSH	Secure Shel
OSPF	Open Shortest Path First
LAN	Local Area Network
IP	Internet Protocol
VLAN	Virtual LAN
ARP	Address Resolution Protocol
MAC	Media Access Control
LLDP	Link Layer Discovery Protocol
API	Application programming interface
GUI	graphical user interface – grafické užívateľské rozhranie

Zoznam príloh

A Zdrojové súbory

A.1 Konfiguračné súbory

B Checklist